Fachhochschule Wedel
Prof. Dr. Sebastian Iwanowski

26.08.2011

Aufgaben zur Klausur in *Computer-Algebra* (SS 2011)

Zeit: 100 Minuten

erlaubte Hilfsmittel: Taschenrechner

Bitte tragen Sie Ihre Antworten und fertigen Lösungen auf gesonderten karierten Blättern ein. Markieren Sie klar, welche Lösung zu welcher Aufgabe gehört und als solche gewertet werden soll. Nicht zu wertende Passagen sind durchzustreichen.

Notizen auf diesem Aufgabenblatt werden grundsätzlich nicht gewertet!
Vergessen Sie nicht, das Deckblatt zu unterschreiben.

Für die Prüfung werden insgesamt 40 Bewertungseinheiten (BE) vergeben. Zum Bestehen benötigen Sie mindestens 20 BE.

Viel Erfolg !

Aufgabe 1: Ganzzahlarithmetik (5 BE)

a) Nennen und begründen Sie die asymptotische Laufzeit der Addition und die der Multiplikation nach der Schulmethode für beliebig lange ganze Zahlen. Geben Sie genau an, von welcher Größe diese Laufzeit abhängt. (2 BE)

b) Skizzieren Sie die Idee, wie der Algorithmus von Karatsuba die Laufzeit für die Multiplikation verbessert. Die genauen Berechnungen müssen Sie dazu nicht angeben. Schildern Sie aber die entscheidenden Einsparungen und nennen Sie die konkrete asymptotische Laufzeit. (3 BE)

Aufgabe 2: Modulare Arithmetik (6 BE)

a) Welche Eigenschaft beschreibt der Kleine Satz von Fermat für eine Zahl n? (1 BE)

b) Charakterisieren Sie genau die Zahlen n, für die diese Eigenschaft gilt! Es reicht für die Ausnahmefälle nicht aus, sie mit einem Namen zu versehen. Nennen Sie konkret die Zerlegungseigenschaft dieser Zahlen. (2 BE)

c) Was ist ein Fermatscher Zeuge für eine Zahl n? (1 BE)

d) Was wissen Sie von n, wenn n einen Fermatschen Zeugen besitzt, und was wissen Sie von n, wenn n keinen Fermatschen Zeugen besitzt? (2 BE)

Aufgabe 3: Modulare Arithmetik (8 BE)

Betrachten Sie in Z_{11} den modularen Logarithmus zur Basis 3:

a) Geben Sie $\log_3 n$ für alle $n \in Z_{11}$ an, für die Lösungen existieren (geben Sie bei Mehrdeutigkeit alle Lösungen an!) und geben Sie die Zahlen $n \in Z_{11}$ an, für die keine Lösung existiert. Begründen Sie das durch eine Rechnung, aus der Sie alle Antworten ableiten können! (3 BE)

b) Warum sind modulare Logrithmen in der Kryptographie interessant? (1 BE)

c) Benennen Sie ein Verfahren und skizzieren Sie seine Funktionalität und seinen Ablauf, das von Ihrer in b) gegebenen Antwort Gebrauch macht! (4 BE)

Aufgabe 4: Polynomarithmetik (6 BE)

a) Erklären Sie das Prinzip der Stützstellentransformation, um die Multiplikation von 2 rationalen Polynomen p(x) und q(x) zu berechnen. (3 BE)

b) Wie gut kann die Laufzeit bestenfalls werden, wenn es keinen Zusammenhang zwischen den Funktionswerten der Stützstellen gibt? Geben Sie die Größe genau an, von der die Laufzeit abhängt. (1 BE)

c) Warum kann die Schnelle Fouriertransformation diese Laufzeit verbessern? Erläutern Sie in Stichworten den algebraischen Hintergrund (der Algorithmus muss nicht angegeben werden!) und nennen Sie die Laufzeit! (2 BE)

Aufgabe 5: Polynomiale Gleichungssysteme (7 BE)

Lösen Sie folgendes Gleichungssystem mit dem Resultantenverfahren:

$x^2 + y = 0$

$x^3 + 2y + 1 = 0$

Hierfür reicht es nicht aus, dass Sie eine gültige Lösung angeben: Sie sollen auch die Zwischenschritte beschreiben, die das Resultantenverfahren nimmt. Beschreiben Sie dafür auch explizit die Zwischenschritte, die sich aus Matrizenumformungen ergeben.

Hinweis für den Lösungsweg: y = -1 ist eine Teillösung, die zum Ziel führt.

Aufgabe 6: Polynomfaktorisierung (5 BE)

a) Geben Sie an, über welchem Zahlenbereich der Algorithmus von Kronecker Polynome korrekt faktorisieren kann! Welche Eigenschaft dieses Zahlenbereichs nutzt der Algorithmus aus? (2 BE)

b) Welche Laufzeit hat der Algorithmus in Abhängigkeit von welchen Größen? (1 BE)

c) Wie kann man mit Hilfe des Algorithmus von Kronecker rationale Polynome faktorisieren? Skizzieren Sie in Worten, welche prinzipiellen Schritte dazu nötig sind.(2 BE)

Aufgabe 7: Polynomfaktorisierung (3 BE)

a) Das Polynom $1 + x^3 + 8x^6$ soll in $\mathbb{Z}_3$ faktorisiert werden. Warum kann es nicht mit dem Algorithmus von Berlekamp faktorisiert werden, und warum versagt die Methode über Ableitungen? (2 BE)

b) Geben Sie die Lösung von a) an! (1 BE)